1   # Smart Grid Architecture Committee Standard Review Form

Standard Name	Guidelines for. Smart Grid Cyber Security
Standard Number	NISTIR 7628 volumes 1, 2, & 3
Standard Development Organization	National Institute of Standards and Technology (NIST)
Document Type (as defined by Standard organization)	Interagency Report
Priority Action Plan	NA
URI to Specification	http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

2

3   *1. Scope as stated in the Standard:*

4   The three-volume report, NISTIR 7628, Guidelines for Smart Grid Cyber Security1, presents an
5   analytical framework that organizations can use to develop effective cyber security strategies
6   tailored to their particular combinations of Smart Grid-related characteristics, risks, and
7   vulnerabilities. Organizations in the diverse community of Smart Grid stakeholders—from
8   utilities to providers of energy management services to manufacturers of electric vehicles and
9   charging stations—can use the methods and supporting information presented in the report as
10 guidance for assessing risk, and then identifying and applying appropriate security requirements
11 to mitigate that risk. This approach recognizes that the electric grid is changing from a relatively
12 closed system to a complex, highly interconnected environment. Each organization's cyber
13 security requirements should evolve as technology advances and as threats to grid security
14 inevitably multiply and diversify.

15 *2. Purpose as stated in the Standard:*

16 Under the Energy Independence and Security Act (EISA) of 2007, the National Institute of
17 Standards and Technology (NIST) has "primary responsibility to coordinate development of a
18 framework that includes protocols and model standards for information management to
19 achieve interoperability of smart grid devices and systems…"

20 Effective cyber security is integral to achieving a nationwide Smart Grid, as explicitly recognized
21 in EISA.2

22   *It is the policy of the United States to support the modernization of the Nation's*
23   *electricity transmission and distribution system to maintain a reliable and secure*

| 24 | *electricity infrastructure that can meet future demand growth and to achieve each of the* |
| 25 | *following, which together characterize a Smart Grid:* |

| 26 | *(1) Increased use of digital information and controls technology to improve reliability,* |
| 27 | *security, and efficiency of the electric grid.* |

| 28 | *(2) Dynamic optimization of grid operations and resources, with full cyber-security.* |

| 29 | **3. *Are the scope and purpose aligned with the actual standard?*** |

30	The Report provides a comprehensive catalogue of the different types of cyber threats that
31	practitioners should be aware of as the current grid is evolved into a smart grid. It does not
32	provide a map of how to address each issue, as it shouldn't, but does provide a nomenclature to
33	describe the threats and a check-list for completeness.

| 34 | Volume 2 catalogues concerns related to personal privacy in residences touched by the smart |
| 35 | grid. |

36	The report does not address whether some issues should present themselves under the model
37	Architecture for the smart grid. Better architectural segmentation of the smart grid will change
38	praxis, and thus invalidate some portions of this report for future work.

39	Many issues facing current installations would present themselves differently if the architecture
40	outlined in the various reference architectures were in place. Not all interactions need to be
41	hard-wired. There are limited number of interactions, such as domain-required timing, wherein
42	future choices will remain constrained. Other interfaces can and will be implemented in several
43	ways.

44	This report provides design guidance, rather than mandating specific design. Users of this report
45	will be aware of issues that arise with current design and deployments, and it should be read
46	with this in mind.

47	The SGAC should use this report to draw its own attention to areas wherein the deployed
48	architecture itself creates the security issues catalogued, and use that to improve and accelerate
49	its own work. This can then provide guidance back to assist the Cybersecurity team to provide
50	more directed advice in future versions.

| 51 | The actual report does address the scope and purpose it title suggests. |

| 52 | **4. *SGAC team summary of purpose and scope*** |

| 53 | The report provides a comprehensive catalogue of the interactions of systems being deployed |
| 54 | today. For each item in the catalogue, the interactions that a cyber-security plan should address |

55   are named. The report catalogues the systems of the day, without looking to the architecture
56   planned for tomorrow's systems.

57   **5. What Conceptual Model Domains are affected:**

Markets	Y
Operations	Y
Service Providers	Y
Bulk Generation	Y
Transmission	Y
Distribution	Y
Customer	Y

58

59   **6. What Levels in the ISO 7 Layer Model and/or the GWAC Stack are affected by the standard?**

Application	
Presentation	X
Session	X
Transport	X
Network	X
Data Link	X
Physical	X

60

61
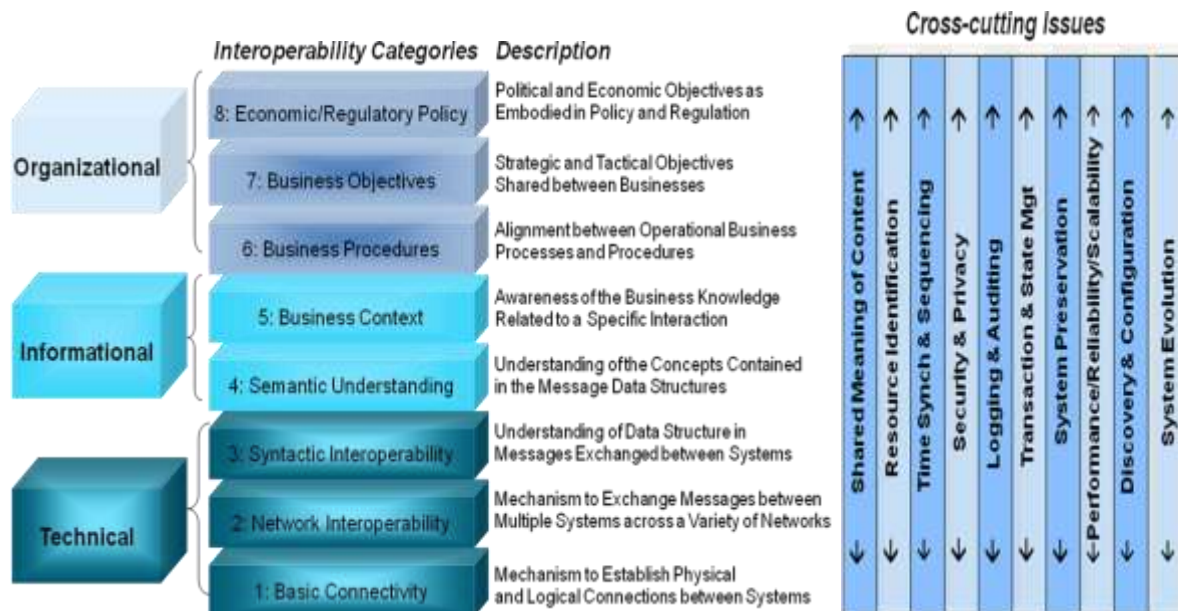
62 The report addresses potentially every level of the GWAC stack, because it addresses security
63 (levels 1-7) and privacy (5-8).

64 **7. If the standard addresses multiple layers… Why? Is there effective separation of layers (in the**
65 **ISO or GWAC stack)? Is there a plan to migrate to single layer standard?**

66 Security is cross-cutting, and failure of security at any level, whether interference with signal,
67 interception of message, or misuse of information is of concern to cyber security. There is no
68 plan to migrate to a single level standard.

69 **8. How would technology based on the standard be used in applications in the future? Adapted**
70 **to today's applications?**

71 The report is well adapted to improving the cyber security of current systems and the ones soon
72 to be deployed. The report was developed independent to the reference architecture (s) for the
73 smart grid and therefore has some areas that should be made in better alignment to support
74 future systems and business models.

75 **9. Is there a migration path from current use in the area of the standard to this standard?**

76 The primary use of this report is to support movement from today's current usage to more
77 secure deployments.

78 **10. Does this standard affect any other PAP (if yes, list)?**

79 The advice and catalogue of issues in NISTIR 7628 apply to all information exchanges,
80 communications protocols, and business processes of the smart grid. This means they apply to
81 most PAPS already formed or that will be formed hereafter.

82 **11. Has this cross PAP effect been discussed by the SGAC evaluation team?**

83 Yes, this cross-PAP effect has been discussed.

84 **12. What action items resulted from team discussions?**

Action Item	Assigned to	Status
None		

85 (Add rows as needed)

86

87	**13. If there are use cases related to the standard, are the use cases and the standard aligned? Are**
88	**these current/past use cases? Are they white box/black box? Are there future use cases or**
89	**requirements?**

90   Much of this report is a catalogue of use cases, i.e., interactions and potential security risks. A
91   potential concern with this report potential misuse. In a regulated market such as that for
92   energy, a description can turn, by regulatory reference, into a requirement.

93   As the Architecture develops, recognition of some of the vulnerabilities identified herein may
94   eliminate some or modify some interactions. Communication of that developing Architecture
95   back to the Cybersecurity Team will then provide more concrete guidance for future
96   implementations.

97   This report must communicate issues with legacy technology and installations even as it looks to
98   the future. Some issues in legacy systems will not be solved while those systems and
99   technologies persist.

100   In a future version of this report (work on which begins soon), it would be useful to identify
101   interactions and associated risks based on the developing architecture, and encourage
102   practitioners to move with all due speed to new applications that are secure by design..

103   **14. If there are use cases, are they candidates for the Conceptual Architecture – Requirements**
104   **Document? If not present, what new requirements may need to be added?**

105   No new use cases for the conceptual architecture were discovered in this report.

106   **15. Is the terminology reasonably understandable by the intended audience? Is the terminology**
107   **consistent through the document? Are standard dictionary(ies) referenced normatively?**

108   The report uses common language well understood in the industry. Most terms are defined
109   within charts and columns that themselves serve as a dictionary to eliminate ambiguity.

110   **16. If UML class or other diagrams are useful for understanding the standard, are they available or**
111   **used in the standard?**

112   Not applicable

113   **17. Does the standard include transitional artifacts? If so, are the transitional artifacts necessary**
114   **to support legacy applications? Can they ever go away?**

115   The security architecture is not attempting to define future business practices, but to apply
116   security to existing and probable future business practices. As such, it codifies issues that persist
117   as long as current systems and business practices exist.

| 118 | A future update to the report would be better if it identified business practices that, from a |
| 119 | security perspective, would be candidates for transition. |

18. Are there things in the standard that have no obvious purpose in the use of the standard? Why do we think they're there? Are those things supporting evolution of application architectures?

There are no aspects with no obvious purpose in the report.

19. This standard is:

A. A new standard that is being created by a new working group

B. A new standard that is being created by a new working group

C. A new standard that is being created by an established working group

D. A standard that was in draft form, but not finalized yet

E. A standard that was released but does not have a testing and conformance plan

F. A standard that is released, has a testing and conformance plan, but is undergoing a major revision

G. A standard that is mature, has testing and conformance and no major revisions are pending

The report is a catalogue of issues and potential security issues. It might be similar to [C], but the categories do not readily apply.

20. Does this Standard limit options for innovation in the future? How? If yes, what limits are placed on innovation?

Two significant purposes of the Architectures of the SG are to reduce attack surfaces and to reduce dependencies between applications and functions. By cataloging end-to-end issues linked to existing business models, the report potentially limits newer solutions which do not have the same end-to-end issues.

The report identifies some issues which are tied to particular market structures and current praxis. As long as the reader takes these as information about issues rather than requirements for future applications, then they will not inhibit innovation. The Cybersecurity committee has made note of those pointed out during this review, and plans to minimize these in future versions.

In particular, some current business practices prohibit sharing information in ways that would ease the entrance of new participants; these are catalogued in this report. Such sharing of information may be the essence of successful future smart energy deployments. There are use

149   cases for live exchange of energy usage within the building, as well as a PAP (17) whose sole
150   purpose is to codify such exchanges. Other applications, and other business models, or even
151   other regulations may encourage or mandate sharing similar information. An exclusive focus on
152   the security aspects of sharing under current business models might discourage the
153   development of innovative technologies and business processes.

154   **21. Other Comments:**

155   Specific architectural concerns which should be addressed in the next version.

156   *Comments on Volume 1L High Level Requirements*

157   Comments on Figure 2-3, Logical Reference Model

158   - U56 appears to penetrate the ESI to perform cross-domain direct control. This is a logical
159   interaction and not a direct one.

160   - 25L Distributed Generation and Storage Management should be either behind a premises
161   ESI or use its own restricted ESI.

162   - U70 penetrates the ESI to perform direct plant control. This is a logical interaction and not a
163   direct one.

164   - There appear to be many direct interactions on the left side of 41 (Aggregator / Retail
165   Energy Provider). While these are intended to be logical, the graphic could be
166   misinterpreted. Work in PAP09 states that all such interactions should be mediated through
167   ESI and must support recursion.

168   - Need definition of ESI for U11 (DR management to Distribution Management)

169   - U106 appears to bypass the premises ESI to interact directly with Customer Energy
170   Management System. While these are logical interactions, it should be noted that making
171   them direct introduces additional security concerns and violates the consensus from PAP09
172   that all such interactions should be mediated through ESI.

173   Comment on Key Concepts and Assumptions

174   - Implied hierarchy in availability and resilience eliminates potential peer to peer negotiations
175   between microgrids. Microgrid models (see Galvin "Perfect Power"--
176   http://www.galvinpower.org/) suggest that availability starts in a local microgrid and that
177   resilience is gained by aggregating and interconnecting those microgrids. The reviewer has
178   spent much of his career operating inside such a microgrid, and knows these interactions

| 179 | are not just theoretical. We suggest that a future version include a section that addresses |
| 180 | security and resilience from the bottom-up microgrid perspective as well. |

| 181 | Comments on Table 2-2, Logical Interfaces |

182	-	Interface 10, interactions between control systems and non-control corporate systems uses
183		as its sole example the interaction between two non-control systems (GIS and Work
184		Management) in the same organization. Wide Area situation awareness is often shared
185		between business entities; such information should be specified and secured in accord with
186		principles of SOA Security. Examples of such interactions might include exchange of WASA
187		between provider and aftermarket consumer (Coop or Aggregator), between Utility and
188		Emergency Management, or between adjacent bulk providers.
189	
190		The SGAC would like to see a future version of this report extend the security analysis to
191		include cases where the information exchanges cross organizational boundaries.

| 192 | - | Interface 17: see comments on Interface 10. |

| 193 | Comments on section 2.3.5 – Logical Interface Category 9 |

194	-	Recommends that the assumptions in Bullet 9 be examined to include scenarios including
195		dynamic discovery of markets, dynamic entry into markets, and dynamic exit from markets.
196		While such activities are prohibited by today's market rules, they may be required to
197		support microgrids, are anticipated by specifications already accepted into the catalog of
198		standards.

| 199 | Comments on section 2.3.8 –Logical Interface Category 12 |

| 200 | - | See comments on figure 2-13, GIS above. |

| 201 | Comments on section 2.3.12 – Logical Interface Category 16 |

| 202 | - | Bullet 4: describes securing knowledge of interactions and information within a microgrid |
| 203 | | from that microgrid. |

204		*Some information exchanged among different appliances and systems must be treated*
205		*as confidential and private to ensure that an unauthorized third party does not gain*
206		*access to it. For instance, energy usage statistics from the customer site that are sent*
207		*through the ESI/HAN gateway must be kept confidential from other appliances whose*
208		*vendors may want to scavenge this information for marketing purposes.*

| 209 | | This is architecturally problematic because it violates the minimal interaction rule while |
| 210 | | blocking the ability of a microgrid to control and manipulate its own resources. The |

211   premises / microgrid executes its internal commands and owns its internal data, and can
212   share it as it wills. Propose that a future version modify this bullet similar to:

213   *Some information exchanged among different appliances and systems must be treated*
214   *as confidential and private to ensure that an unauthorized third party does not gain*
215   *access to it. For instance, energy usage statistics from the customer site that are sent*
216   *through the ESI/HAN gateway must be kept confidential.*

217   This removes what appears to be a blanket prohibition on internal [to the
218   premises/microgrid] access to operational information

219   -   Many bullets suggest multiple "through the interface" interactions. While this describes the
220   interactions of today, the mode of design creates the possibility of multiple security issues.
221   We recommend that a future version of the report note this issue, and recommend that
222   new implementations minimize such interactions.

223   **22. SGAC Summary Comments:**

224   At the highest level, the architecture of the smart grid is segmented into the domains
225   Operations, Markets, Service Provider, Customer, Generation, Transmission, Distribution, and
226   Customer. To the extent possible, these domains communicate with each other through
227   minimal messages, and have minimal interactions across the inter-domain boundaries. This
228   architecture is necessary to support the growing diversity of technology and process that is both
229   a necessary enabler and a result of the rapid innovation needed to meet national goals.

230   Architecturally, the answer to this challenge is to limit direct interactions across each interface
231   between domains.

232   *Interacting with Line of Business Applications*

233   While core grid operations and interactions draw the most attention, the focus of the
234   architecture on service interactions has implications for other areas of traditional "Utility
235   Applications". These applications do and will exist for a long time.

236   The SGAC recommend that a future version of the report make recommendations about
237   componentizing these applications in place to support better security over their life-times. For
238   example, best practices in service oriented enterprises are to move toward common
239   authentication and authorization mechanisms. These approaches are necessary at the
240   intersection of Architecture and Security.

241   *Interacting with GIS Systems*

242   NISTIR 7628 sketches numerous interactions between GIS systems and line of business
243   applications. Situation awareness on the grid involves collection and analysis of multiple rapidly
244   changing datasets that are or can be tagged with geospatial positions.

245   The SGAC recommends that a future version of report reference existing work on Security in
246   distributed GIS systems that can be found in the Open Geospatial Consortium (OGC), especially
247   in interagency information sharing and in emergency management.

248   Users of the NISTIR working with geospatial systems may wish to review OGC work on sharing
249   geospatial data and wide-area situation awareness. Just as in the NISTIR, the OGC does not
250   endorse any particular approach, but tests test and document various best practices related to
251   the OGC web services (and encodings) in various security environments.

252   2009   Geospatial eXtensible Access Control Markup Language (GeoXACML):
253   http://www.opengeospatial.org/standards/geoxacml This is an OGC standard.

254   2011   OGC Authentication Interoperability Experiment
255   http://www.opengeospatial.org/projects/initiatives/authie (overview)
256   http://portal.opengeospatial.org/files?artifact_id=41734 (report)

257   2009   OWS-6 Secure Sensor Web Engineering Report
258   http://portal.opengeospatial.org/files/?artifact_id=34273 - This Engineering Report
259   introduces standards-based security solutions for making the existing OGC Sensor Web
260   Services, as described in the OWS-6 SWE baseline, ready towards the handling of
261   sensors in the intelligence domain.

262   2009   OWS-6 Security Engineering Report:
263   http://portal.opengeospatial.org/files/?artifact_id=35461
264   This Engineering Report describes work accomplished during the OGC Web Services Test
265   bed, Phase 6 (OWS 6) to investigate and implement security measures for OGC web
266   services. This work was undertaken to address requirements stated in the OWS-6
267   RFQ/CFP originating from a number of sponsors, from OGC staff, and from OGC
268   members.

269   2010   OWS-7 - Towards secure interconnection of OGC Web Services with SWIM:
270   http://portal.opengeospatial.org/files/?artifact_id=40144
271   This Engineering Report provides guidance and generate action items for the OGC
272   standardization effort to properly enable security in the near future such that a
273   seamless, interoperable but secure interconnection between OGC Web Services and
274   FUSE ESB technology stack as selected by use in the System Wide Information
275   Management (SWIM) System of the US Federal Aviation Administration (FAA) can be
276   achieved.

277	2007:	Trusted Geo Services IPR: http://portal.opengeospatial.org/files/?artifact_id=20859
278		The OGC Trusted Geo Services Interoperability Program Report (IPR) provides guidance
279		for the exchange of trusted messages between OGC Web Services and clients for these
280		services. It describes a trust model based on the exchange and brokering of security
281		tokens, as proposed by the OASIS WS-Trust specification [http://docs.oasis-
282		open.org/ws-sx/ws-trust/200512].